UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

| | | |
|---|---|---|
| *Jessica Leah Kampschroer and Corey Patrick Kampschroer* | ) | Case No. 13-cv-2512 (SRN-TNL) |
| *Plaintiffs,* | ) | |
| *v.* | ) | |
| *Anoka County et al.* | ) | |
| *Defendants.* | ) | |

**STATE DEFENDANTS' MEMORANDUM IN SUPPORT OF THEIR MOTION TO DISMISS**

The Minnesota Department of Public Safety ("DPS") makes driver's license data available to law enforcement agencies through a computerized database. The database is an essential law enforcement tool, providing law enforcement officers with timely access to information that is vital to their activities. Plaintiffs allege that various local law enforcement officers used the database to access their driver's license data without proper purpose, in violation of the Driver Privacy Protection Act ("DPPA") and their constitutional right of privacy. Plaintiffs sue the officers who accessed the data (as John and Jane Doe defendants), their employers, and three DPS officials – current Commissioner Ramona Dohman, prior Commissioner Michael Campion, and Director of Driver and Vehicle Services Pat McCormack.[1]

[1] Collectively, Defendants Campion, Dohman, and McCormack are hereinafter referred to as the "State Defendants".

Plaintiffs fail to state a claim against the State Defendants. Plaintiffs' claims against the State Defendants are identical to claims that Judge Ericksen recently considered and dismissed in another case, *Kiminski et al. v. Hunt, et al.*, Case No. 13-185. *See* Docket Entry No. 30, *Kiminski et al. v. Hunt, et al.*, Case No. 13-185, D. Minnesota (September 20, 2013) (attached hereto as Exhibit A.) As Judge Ericksen correctly held, DPS officials are not liable for the misuse of the DPS driver's license database by law enforcement personnel. Liability for such misuse, if it exists, is with the law enforcement officers who misused the data, not with DPS officials.

**BACKGROUND**

Plaintiffs, Jessica Leah Kampschroer and Corey Patrick Kampschroer, bring suit against the State Defendants, along with a number of counties and municipalities, for the conduct of law enforcement officers in allegedly accessing their driver's license data without proper purpose. (Compl. pp. 3-4.) Defendants Dohman and Campion are the current and immediately preceding DPS Commissioners. (*Id.* ¶¶ 158-159.) Defendant McCormack is the current DPS Director of Driver and Vehicle Services. (*Id.* ¶ 160.) Defendant Dohman is sued in her individual and official capacities. (*Id.* ¶159.) Defendants Campion and McCormack are sued in their individual capacities. (*Id.* ¶¶ 158, 160.)[2]

[2] Plaintiffs also name John and Jane Doe defendants working for DPS, but do not plead sufficient detail to identify who they are, or if they even exist. (Compl. ¶ 162.) Plaintiffs' theory of liability with respect to the Doe defendants is the same as their theory of liability with respect to the State Defendants. As a result, if the Court dismisses the State Defendants, it should also dismiss the DPS Doe defendants.

## ARGUMENT

### I. THE COURT SHOULD FOLLOW THE HOLDINGS OF JUDGE ERICKSEN IN *KIMINSKI* AND DISMISS THE STATE DEFENDANTS FROM THIS SUIT.

As the Court is likely aware, this is one of a succession of recently filed cases alleging that DPS officials are personally liable for the alleged improper use of driver's license data by law enforcement officers or other government employees pursuant to the DPPA and constitutional right of privacy.[3] The complaints in each case are substantively identical.[4] In *Kiminski*, Judge Ericksen correctly dismissed these claims, holding that DPS officials cannot be held not liable for their alleged failure to prevent improper use of the DPS driver's license database.

The *Kiminski* plaintiffs are a putative class of persons who alleged that their driver's license data was improperly accessed by Department of Natural Resources' employee John Hunt. (*Kiminski* Order, p. 1.) The *Kiminski* plaintiffs sued Commissioners Dohman and Campion, among others, alleging they are personally liable for giving Hunt access to the DPS driver's license database. (*Id.* p. 3.) Judge Ericksen dismissed the Commissioners from all counts pled against them.

---

[3] Other cases in which DPS officials are currently named as defendants in suits pleading the same causes of action pled here include: *Kiminski v. Hunt*, 13-cv-195; *Kost v. Hunt*, 13-cv-583; *Bass v. Anoka County*, 13-cv-860; *Brian Potocnik v. Anoka County*, 13-cv-1103; *Gulsvig v. Peterick*, 13-cv-1309; *McDonough v. Al's Auto Sales*, 13-cv-1889; *Sheila Potocnik v. Carlson*, 13-cv-2093; *Loeffler v. City of Anoka*, 13-cv-2093; *Mallack v. Aitkin County*, 13-cv-2119; *Nelson v. Schlener*, 13-cv-340; and *Rochen v. Wabasha County*, 13-cv-2490. In addition, DPS officials were originally named, then dismissed pursuant to settlement, in *Rasmussen v. Bloomington*, 12-cv-632, a case still pending before this Court.

[4] For comparison, a copy of the *Kiminski* complaint is attached hereto as Exhibit B.

With respect to the DPPA, Judge Ericksen held that DPS officials cannot be held liable merely for giving state and local government employees access to the DPS driver's license database, even if the DPS officials failed to adequately monitor or control use of the database. (*Id.* pp. 8-16.) In *Kiminski*, as in this case, the plaintiffs made two arguments concerning why DPS officials could be held liable for the improper use of the DPS driver's license database by others. (*Id.* p. 9.) First, the plaintiffs argued that the DPPA makes DPS officials liable even if they did not know of Hunt's improper use of the database, as long as they knowingly gave Hunt access to the database. (*Id.*) Judge Erickson rejected this argument, holding that the DPPA's use of the word "knowingly" makes a disclosure of driver's license data actionable only where the individual disclosing the data knows that a disclosure is being made *and* knows that the recipient is using the data for an improper purpose. (*Id.* pp. 10-13.) Second, the *Kiminski* plaintiffs argued that the DPPA makes DPS officials liable for granting law enforcement officers access to the DPS driver's license database without adequate monitoring and control. (*Id.* p. 9.) Judge Ericksen rejected this argument, holding that the DPPA does not create a private right of suit for alleged negligence or mismanagement of driver's license data by state officials. (*Id.* pp. 13-16.)

With respect to the constitutional right of privacy, Judge Ericksen held that driver's license data is not the type of highly sensitive information afforded protection

under the constitutional right of privacy, and therefore dismissed the plaintiffs' constitutional claims. (*Id.*, pp. 24-26.)[5]

This Court should follow Judge Ericksen's holdings on the legal issues and dismiss the State Defendants from this suit. The allegations of the *Kiminski* complaint and the present complaint are substantively identical. Indeed, the *Kiminski* plaintiffs were represented by the same counsel as the present defendants, and much of the present complaint is lifted verbatim from the *Kiminski* complaint. The arguments the parties will make to this Court are the same arguments the parties made in *Kiminski*. Judge Ericksen's ruling is a thorough and well-reasoned analysis of these issues. In addition, following Judge Ericksen's rulings on the interpretation of the DPPA and constitutional right of privacy avoids creating a potential split in authority within this district on these issues, which is particularly important given large the number of simultaneously proceeding cases making identical claims.

As further set forth below, Judge Ericksen's decision is *Kiminski* is also the correct interpretation of the applicable law.

## II. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE DPPA.

The DPPA is a limited statute. It grants limited protections to driver's license information, and a limited right of private suit only against persons who knowingly obtain, disclose, or use driver's license data for an improper purpose.

---

[5] Judge Ericksen also accepted the Commissioners' argument, set forth in Section V of this memorandum, that DPPA claims must be brought exclusively under the provisions of the DPPA itself, and cannot be brought under Section 1983. (Ex. A. pp. 19-24.)

Plaintiffs do not allege that the State Defendants personally obtained, disclosed or used Plaintiffs' driver's license data, let alone for an improper purpose. Plaintiffs instead plead that the State Defendants are liable merely for giving law enforcement officers access to the DPS driver's license database, or alternatively, for failing to prevent the misuse of the database by those officers. As Judge Ericksen held, these arguments are contrary to the plain language of the DPPA, as well as the purpose and intent of the act.

**A. Background Of The DPPA.**

The DPPA was passed in 1994 in response to the murder of actress Rebecca Schaefer by a stalker who had obtained her unlisted home address from the California Department of Motor Vehicles. Maureen Maginnis, *Maintaining the Privacy of Personal Information: The DPPA and the Right of Privacy*, 51 S.C. L. Rev. 807, 809 (2000). As a result, the scope of the DPPA is narrow, designed to deny access to driver's license data "only . . . to a narrow group of people that lack legitimate business," while permitting access by people with legitimate need for the data. *Cook v. ACS State & Local Solutions, Inc.*, 663 F.3d 989, 995-96 (8th Cir. 2011) *quoting* 140 Cong. Rec. 7929 (statement of Rep. Goss).

The DPPA broadly permits disclosure of driver's license data to law enforcement, government agencies, auto dealers, civil litigants, academic researchers, insurers, private investigators, and many others. 18 U.S.C. § 2721(b). As originally passed, the DPPA even permitted disclosure to direct marketing firms unless the driver specifically opted out. *Id.* The DPPA was only later amended to require the driver to "opt-in" before permitting disclosure to direct marketers. *Id.* The DPPA additionally permits States to

sell driver's license data to third parties such as Westlaw for further dissemination to permitted users. 18 U.S.C. § 2721.

The DPPA does not mandate the manner in which driver's license information is stored, handled, maintained, or supervised. There are no implementing federal regulations concerning the handling of driver's license data under the DPPA. The absence of such regulations is in stark contrast to federal privacy statutes. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and associated regulations contain detailed provisions regulating the storage and transmission of health data, as well as specific oversight requirements for supervisors. *See*, *e.g.*, 45 C.F.R. § 164.308.[6]

The DPPA's right of private suit is also narrow, permitting suits only against "persons" who "knowingly" and improperly obtain, disclose or use driver's license data:

> A *person* who *knowingly obtains, discloses or uses personal information*, from a motor vehicle record, *for a purpose not permitted under this chapter* shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court

18 U.S.C. § 2724 (emphasis added). The DPPA specifically exempts States and State agencies from the definition of "persons" who may be privately sued. 18 U.S.C. § 2725(2). Instead, the DPPA confers the exclusive authority to take action against State departments of motor vehicles on the United States Attorney General:

---

[6] Among other things, the HIPPA regulations require that entities in possession of health data conduct risk assessments, implement security measures, audit access to information, and compartmentalize access. 45 C.F.R. § 164.308.

> Any State department of motor vehicles that *has a policy or practice of substantial noncompliance with this chapter* shall be subject to a civil penalty imposed by the *Attorney General* of not more than $5,000 a day for each day of substantial noncompliance.

18 U.S.C. § 2723 (emphasis added).

### B. The State Defendants Are Not Liable For The Misuse Of The DPS Driver's License Database by Others.

Plaintiffs claim that the State Defendants can be held liable under the DPPA simply because they oversaw the administration of the DPS driver's license database. (*See*, *e.g.*, Compl. ¶¶ 343-354, 478.) These allegations do not state a claim under the DPPA, which imposes liability only if the defendant "knowingly obtains, discloses or uses" such data for a "purpose not permitted" by the act. 18 U.S.C. § 2724. The State Defendants must therefore be dismissed.

#### 1. Plaintiffs have not pled a cause of action against the State Defendants.

As discussed above, the narrow private cause of action under the DPPA applies to "[a] person who *knowingly obtains, discloses or uses* personal information, from a motor vehicle record, *for a purpose not permitted under this chapter*." 18 U.S.C. § 2724 (emphasis added). Plaintiffs do not allege any act by the State Defendants that falls within the limited scope of this provision. Plaintiffs do not allege that the State Defendants personally obtained, disclosed, or used their driver's license data, let alone for a "purpose not permitted."

The DPPA expressly permits disclosure of driver's license data to law enforcement officers. 18 U.S.C. § 2721(b)(1). As Judge Ericksen held in *Kiminski*,

granting law enforcement officers access to the DPS Driver's license database therefore cannot not, in and of itself, constitute a violation of the DPPA:

> Plaintiffs' contention that the State Defendants' culpable act was granting Hunt database access fails to state a claim for relief under the DPPA for a straight-forward reason: the complaint alleges no facts that make it plausible that the defendants "knowingly" gave defendant Hunt database access "for a purpose not permitted" by the DPPA. At no point does the complaint allege that Defendant Hunt should not have received access to the DPS Databases for purposes of his legitimate job duties as a DNR employee. The list of permissible uses of personal information under the DPPA covers the operations of the DNR. *See* 18 U.S.C. § 2721(b)(1) ("For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions."). The complaint acknowledges that at all material times, Defendant Hunt was an employee of the DNR. It alleges that he was the administrative manager of the DNR's enforcement division, was among those in charge of open records and data training at the DNR, and handled public requests for records as a data compliance officer at the DNR. These alleged facts imply that the State Defendants gave Defendant Hunt access to the DPS Databases for purposes of performing his job at the DNR. The complaint does not contend otherwise. Under these circumstances, Plaintiffs' complaint fails to state a claim for a DPPA violation by any of the State Defendants.

(*Kiminski* Op. pp. 8-9.) As in *Kiminski*, the present Plaintiffs make no allegation that the law enforcement officers who are defendants in this case were improperly granted access to the DPS Drivers' license database.

To the extent Plaintiffs allege that the State Defendants can be held liable because they knowingly gave law enforcement officers access to the database, even if the Commissioners were unaware of the officers' improper use of the data (*see, e.g.,* Compl. ¶ 381), such allegations cannot sustain a private right of action under the DPPA. (*Kiminski* Op. pp. 10-13.) To hold otherwise would make State officials strictly liable for

the misdeeds of any person who misuses driver's license data obtained from the State. This is inconsistent with the language and intent of the DPPA, which makes only "knowing" disclosures of driver's license data for an improper purpose actionable. (*Id.*) It would also create an unmanageable result. The DPS driver's license database is accessed for legitimate reasons millions of times per year. The DPPA should not be read to create the absurd result of making the State Defendants liable if, among the millions of legitimate queries of the database, some law enforcement officers abuse their access. *See City of Jefferson City, Mo. v. Cingular Wireless, LLC*, 531 F.3d 595, 606 (8th Cir. 2008) (holding federal courts assume legislatures do not intend absurd results when passing statutes); *Foulk v. Charrier*, 262 F.3d 687, 703 (8th Cir. 2001) (same).

Nor do Plaintiffs' allegations of negligent or reckless management or monitoring of the DPS driver's license database save their claim against the State Defendants. The DPPA's use of the word "knowingly" when specifying the conduct actionable by private suit is specific and meaningful. Had Congress intended to impose a negligence or recklessness standard for a private right of action under the DPPA, it would have used those words – as it has done with other similar statutes. For example, with respect to tax records, Congress made the negligent inspection or disclosure of tax records actionable by specifically including the word "negligent" in the statute. 26 U.S.C. 7431(a) ("If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information . . . in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.")

In addition, the DPPA contains no provisions regulating the manner in which driver's license data must be managed.[7] It also contains no provisions making mismanagement of driver's license data actionable by way of private suit. Under the DPPA, only the U.S. Attorney General is authorized to take action for the mismanagement of driver's license information, and only where the State department of motor vehicles has a "policy or practice of substantial noncompliance with [the DPPA]" 18 U.S.C. § 2723(b). The U.S. Attorney General's remedies are also limited to imposing a civil penalty of "not more than $5,000 a day for each day of substantial noncompliance," *id.*, not the various actual, liquidated, or punitive damages and other remedies available to private litigants against a person who actually "knowingly obtains, discloses or uses" driver's license information for an improper purpose. 18 U.S.C. § 2724.

As private litigants, Plaintiffs must therefore plead and prove that the State Defendants personally and knowingly obtained, used, or disclosed Plaintiffs' driver's license data for an improper purpose. Plaintiffs have not and cannot meet this burden.

**2. Even if relevant, Plaintiffs have not sufficiently pled that the State Defendants knew law enforcement officers were misusing the driver's license database.**

In support of their allegations that the DPs Defendants mismanaged access to the driver's license database, Plaintiffs plead "on information and belief" that the State

---

[7] The DPPA thus stands in contrast to other federal statutes in which Congress imposed liability for improperly maintaining information, for example with health information and HIPAA. *See supra* at n.2.

Defendants "knew" of the misuse, and did nothing to stop it. (*See*, *e.g.*, Compl. ¶ 378.) Even assuming that knowledge of misuse of the database would support a private right of action under the DPPA against the DPS Defendants as opposed to civil penalties imposed on DPS by the U.S. Attorney General, Plaintiffs have not sufficiently pled facts to support their allegations that the DPS Defendants knew of such misuse.

In *Bell Atlantic v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal,* 556 U.S. 662 (2009), the Supreme Court abrogated its prior case law on pleading standards, holding that plaintiffs can no longer survive a motion to dismiss with pleadings that simply "[leave] open the possibility that [the] plaintiff might later establish some set of undisclosed facts to support recovery." *Twombly*, 550 U.S. at 561. The Supreme Court now requires plaintiffs to plead facts that "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. The purpose of the Supreme Court's shift in pleading standards is to make clear that notice pleading under Rule 8 "does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions." *Id.*

Here, Plaintiffs employ the exact type of pleading barred by *Twombly/Iqbal* in making only conclusory allegations that the State Defendants "knew" of misuse of the DPS driver's license database by law enforcement officers. Plaintiffs attempt to support these conclusory allegations with assertions that are nothing more than purported biographical information regarding the Commissioner Defendants. (*See*, *e.g.*, Compl. ¶¶

440-450.)[8] These allegations do not show knowledge of law enforcement officers' misuse of driver's license data. As *Iqbal* held, "[t]hese bare assertions, much like the pleading of conspiracy in *Twombly*, amount to nothing more than a 'formulaic recitation of the elements' of a constitutional discrimination claim, . . . As such, the allegations are conclusory and not entitled to be assumed true." 556 U.S. at 681-82 (quoting *Twombly*, 550 U.S. at 555).

## III. PLAINTIFFS FAIL TO STATE A CLAIM FOR A VIOLATION OF THEIR CONSTITUTIONAL RIGHTS.

Plaintiffs plead that the State Defendants violated their Fourth and Fourteenth Amendment Constitutional rights. (*See e.g.* Compl. ¶ 531.) These claims should be dismissed because Plaintiffs cannot meet the threshold requirement of showing that driver's license data is the type of intimate information protected from disclosure by the constitutional right of privacy.[9]

---

[8] Plaintiffs also plead that Commissioner Dohman attended a legislative audit subcommittee hearing in February of 2013 in which misuse of the driver's license database was discussed. (Compl. ¶ 448.) However, all of the alleged DPPA violations pled by Plaintiffs occurred prior to 2012, with the vast majority occurring in 2004-2009. (Compl. Ex. A, B.) Obviously, Commissioner Dohman's presence at a hearing in 2013 cannot support an inference as to her knowledge of misuse of the database from 2004-2011.

[9] To the extent Plaintiffs can make out a claim for a violation of their right of privacy, it must be under the Fourteenth Amendment, not the Fourth Amendment. *See Hurst v. State Farm Mut. Auto. Ins. Co.*, CIV.A. 10-1001-GMS, 2012 WL 426018 (D. Del. Feb. 9, 2012) (recognizing that disclosure of driver's license data did not violate Fourth Amendment because "the Supreme Court has opined that the 'right of privacy' is founded in the Fourteenth Amendment concept of personal liberty, not the Fourth Amendment"). In addition, the State Defendants could not locate any case holding that a disclosure of driver's license data or similar information constituted an illegal search or seizure under the Fourth Amendment.

Right of privacy claims rarely rise to the level of a constitutional violation. *Alexander v. Pfefer,* 993 F.2d 1348, 1350-51 (8th Cir. 1993). As the *Alexander* court held:

> As a preliminary matter we note that tortious conduct even when performed under the color of law does not become a constitutional wrong. "[T]he personal rights found in [the] guarantee of personal privacy must be limited to those which are 'fundamental' or 'implicit within the concept of ordered liberty.'"
>
> ***
>
> Just last term, the Supreme Court reaffirmed its reluctance to expand its concept of substantive due process "because guideposts for responsible decision making in this unchartered area are scarce and open-ended."
>
> ***
>
> [We] have previously rejected claims that the Due Process Clause should be interpreted to impose federal duties that are analogous to those traditionally imposed by state tort law.

*Alexander*, 993 F.2d at 1350 (citing *Paul v. Davis*, 424 U.S. 693 (1976) and *Collins v. City of Harker Heights, Tex.*, 503 U.S. 115, 125 (1992)).

As a result, federal courts have dismissed constitutional privacy claims in all but the most extreme cases involving highly sensitive information. Driver's license data does not meet this standard. *Kiminski* Op. pp. 24-26; *Collier v. Dickinson*, 477 F.3d 1306, 1308 (11th Cir. 2007) (holding that a release of driver's license data did not give rise to a constitutional claim); *see also Condon v. Reno*, 155 F.3d 453 (4th Cir. 1998), *rev'd on separate grounds*, 528 U.S. 141 (2000); *Travis v. Reno*, 12 F. Supp.2d 921 (W.D. Wis. 1998), *rev'd on separate grounds*, 163 F.3d 1000 (7th Cir. 1998); *Pryor v. Reno*, 171

F.3d 1281 (11th Cir. 1999), *vacated on separate grounds*, 211 F.3d 1227 (11th Cir. 2000). Individuals show driver's licenses to prove identity on a regular basis – when entering a bar, or cashing a check, or boarding a plane. Given the frequency with which driver's license data is requested and provided on a day-to-day basis, the disclosure of such information cannot rise to the level of a constitutional violation.

Indeed, federal courts have dismissed cases involving information far more sensitive than driver's license information. In *Alexander*, the defendant sheriff revealed in a radio interview that the plaintiff had failed tests needed to qualify as a police officer. *Alexander*, 993 F.2d at 1349. In *Davis III v. Bucher*, 853 F.2d 718 (9th Cir. 1988), the defendant prison guard circulated nude photographs of an inmate's wife. *Id*. at 719. In *Lambert v. Hartman*, 517 F.3d 433 (6th Cir. 2008), the defendant clerk of court posted the plaintiff's social security number on the internet, resulting in an identity theft. *Id*. at 435. In each of these cases the courts found that the information was not sufficiently sensitive to be a basis for a constitutional violation of the right of privacy. This Court should similarly dismiss Plaintiffs' constitutional claim.

## IV. EVEN ASSUMING, ARGUENDO, THAT PLAINTIFFS HAVE PLED A CLAIM AGAINST THE STATE DEFENDANTS UNDER THE DPPA OR CONSTITUTIONAL RIGHT OF PRIVACY, PLAINTIFFS CANNOT MAINTAIN A SUIT FOR DAMAGES BECAUSE THE STATE DEFENDANTS HAVE QUALIFIED IMMUNITY.

As discussed above, the State Defendants did not violate the DPPA or Plaintiffs' constitutional right of privacy and therefore they should be dismissed from this case. In the alternative, the Court should dismiss the damages claims against the State Defendants based on the doctrine of qualified immunity.

Qualified immunity shields officials, like the State Defendants, from liability for damages for actions taken under color of law unless their conduct "violate[s] clearly established statutory or constitutional rights of which a reasonable person would have known." *Pearson v. Callahan*, 555 U.S. 223, 231 (2009). In *Roth v. Guzman*, 650 F.3d 603, 611 (6th Cir. 2011) the Sixth Circuit applied qualified immunity to damages claims against State officials under the DPPA. *Id.* at 612. The Court should do the same in this case because liability under the DPPA, as pled by Plaintiffs, was not clearly established at the time of the alleged conduct.

The Court should also dismiss Plaintiffs' constitutional claims for damages because there is no clear constitutional right of privacy in driver's license data. *See Kiminski* Op. pp. 24-26; *Collier,* 477 F.3d at 1308*; see also*, *e.g.*, *Tokar v. Armontrout*, 97 F.3d 1078, 1084 (8th Cir. 1996) (applying qualified immunity to claim that disclosure of HIV status violated the plaintiff's constitutional right of privacy); *Bloch v. Ribar*, 156 F.3d 673, 683 (6th Cir. 1998) (applying qualified immunity to claim that disclosure of details of a rape violated the plaintiff's constitutional right of privacy).

In *Bloch*, for example, the plaintiffs were a husband and wife who sued a sheriff for holding a press conference in which he disclosed the details of the wife's rape to the media. *Id.* at 676. The plaintiffs alleged that the sheriff made the disclosure in retaliation for the plaintiffs' public criticism of the sheriff's investigation of the crime. *Id.* The court found that the sheriff had violated the plaintiffs' right of privacy, but nonetheless dismissed the plaintiffs' damages claim because "a reasonable public official would not be on notice that the release of such intimate details of a rape constituted an actionable

violation of a rape victim's privacy interests." *Id.* at 686. As a result, the court held that the sheriff was entitled to qualified immunity. *Id.* at 687.

Driver's license data is far less sensitive than the information disclosed in *Bloch*. Moreover, even under the most favorable view of Plaintiffs' pleading, the State Defendants, unlike the sheriff in *Bloch*, did not intentionally disseminate driver's license information for impermissible purposes, and certainly did not do so for the purpose of retaliating against Plaintiffs. The Court should therefore conclude the State Defendants have qualified immunity from suit for damages.

## V. PLAINTIFFS' SECTION 1983 CLAIM BASED ON ALLEGED VIOLATIONS OF THE DPPA SHOULD BE DISMISSED.

Plaintiffs pleads DPPA claims in two ways. In Count I, they plead a claim directly under the DPPA. In Counts III and IV, they plead a claim under 42 U.S.C. § 1983 for violation of the DPPA. The Court should dismiss the Section 1983 DPPA related claims because, as discussed above, the State Defendants did not violate the DPPA. *See supra*, Section II. In addition, Section 1983 cannot be used to enforce the DPPA.

Not all federal statutes are enforceable through a Section 1983 action. The DPPA may not be enforced under Section 1983 if Congress implicitly foreclosed use of Section 1983 for that purpose by including remedies in the DPPA that are inconsistent with Section 1983 relief. *See*, *e.g.*, *Livadas v. Bradshaw,* 512 U.S. 107, 133 (1994) and *Alexander v. Sandoval,* 532 U.S. 275, 290 (2001) (holding that federal statute may not be enforced through a Section 1983 action where the statute includes provisions for relief that are incompatible with Section 1983).

There is a split in authority whether Congress implicitly foreclosed Section 1983 enforcement of the DPPA. *See Kiminski* Op. pp. 19-24; *see also Roberts v. Source for Pub. Data*, 606 F. Supp. 2d 1042, 1046 (W.D. Mo. 2008) (holding Section 1983 enforcement of the DPPA is implicitly foreclosed); *Kraege v. Busalacchi*, 687 F. Supp. 2d 834 (W.D. Wis. 2009) (same); *Collier v. Dickinson*, 477 F.3d 1306 (11th Cir. 2007) (holding Section 1983 enforcement of the DPPA is not implicitly foreclosed); *Arrington v. Richardson*, 660 F. Supp. 2d 1024 (N.D. Iowa 2009) (same).

To date, Judge Ericksen's opinion in *Kiminski* is the only decision from this District addressing the issue of whether the DPPA implicitly forecloses enforcement through Section 1983. Judge Ericksen correctly concluded that the DPPA does implicitly foreclose suit pursuant to Section 1983. (*Kiminski* Op., pp. 19-24.) The Court should follow the *Kiminski*, *Roberts* and *Kraege* Courts and hold that Congress implicitly foreclosed Section 1983 enforcement of the DPPA.

All five cases cited above conduct the same inquiry, analyzing whether the terms of the DPPA are incompatible with enforcement under Section 1983. The *Kiminski*, *Roberts* and *Kraege* courts correctly concluded that enforcement terms of the DPPA are incompatible with Section 1983. There are at least four ways in which the enforcement provisions of the DPPA are incompatible with enforcement under Section 1983.

First, the DPPA contains criminal penalties, 18 U.S.C. § 2723(a), but Section 1983 does not. Second, unlike Section 1983, the DPPA permits the U.S. Attorney General to enforce the act against States through imposition of civil penalties. 18 U.S.C. §2723(b). Third, the DPPA does not permit a private cause of action against States or State

agencies, 18 U.S.C. § 2724(a), 2725, including for injunctive relief, 18 U.S.C. § 2724(b)(4). By use of official capacity suits, Section 1983 does effectively permit private parties to sue States or State agencies for prospective injunctive relief. Indeed, Plaintiffs seeks official capacity prospective injunctive relief in Count IV of their complaint. Fourth, even the U.S. Attorney General cannot obtain injunctive relief against a State or State agency under the DPPA. 18 U.S.C. § 2723(b).

Given the express remedial provisions of the DPPA, and their inconsistency with Section 1983 forms of relief, Congress must have intended for the DPPA to be enforced only through its own terms. The Court should therefore also dismiss Plaintiffs' Section 1983 claims to enforce the DPPA based on the incompatibility of the DPPA and Section 1983 enforcement provisions.

## CONCLUSION

For the reasons set forth above, the Court should enter an order dismissing the State Defendants, with prejudice.[10]

Dated: October 29, 2013

Respectfully submitted,

OFFICE OF THE ATTORNEY GENERAL
State of Minnesota

s/**Oliver J. Larson**
OLIVER J. LARSON
Atty. Reg. No. 0392946

Assistant Attorney Generals
445 Minnesota Street, Suite 1800
St. Paul, Minnesota 55101-2134
(651) 757-1265 (Voice)
(651) 282-2525 (TTY)

ATTORNEY FOR THE STATE DEFENDANTS

[10] As previously referenced, the Doe defendants should also be dismissed. *See supra*, n.2.